# Solvency answers

## No solvency: Gov’t always finds new authority

New technologies inevitably create new opportunities

Waldman, Sr. Writer at American Prospect, 2015

[Paul, “A reality check on the future of government spying,” Washington Post, 6/3/15]

And let’s not forget that the NSA and other government agencies are certain — not possible, not likely, but certain — to come up with new ways to spy on Americans as new technologies become available. Just as the NSA did with the bulk phone data collection, they’ll probably take a look at earlier laws and decide that there’s a legal basis for whatever new kind of surveillance they want to begin — and that it’s best if the public didn’t know about it. Indeed, just this week an investigation by the Associated Press revealed that the FBI is using aircraft with advanced cameras to conduct investigations without warrants. That’s a relatively mundane use of technology, but there will always be new tools and capabilities coming down the pike, and the impulse will always be to put them into operation, then figure out afterward if it’s legally justifiable. The story of the bulk telephone data collection tells us that the only thing likely to restrain the expansion of government surveillance is public exposure. If you’re hoping that politicians who care about privacy will do it on their own, you’re likely to be disappointed.

## **Most current surveillance occurs entirely outside legal authority**

Patel, co-director Liberty and Natl Security Program at Brennan Center at NYU Law School in 2015

Faiza Patel, The USA Freedom Act marks the beginning, not the end, of the fight to protect our privacy, June 25, 2015 http://america.aljazeera.com/opinions/2015/6/when-will-surveillance-reform-stop-being-just-cool.html#

The vast majority of U.S. surveillance doesn’t take place under any law passed by Congress. When our intelligence agencies collect information overseas — for example, by tapping into fiber optic cables to scoop up all information that flows through them — they operate under an order issued by President Ronald Reagan in 1981, Executive Order 12333, which gives the NSA even greater latitude to collect information with even fewer privacy safeguards than any legislation. Just because information is collected from a cable overseas doesn’t mean that it concerns only foreigners. Purely domestic emails may be routed through another country and picked up. Copies of documents are stored by cloud providers overseas, sometimes in multiple locations. Domestic websites often have ads, pop-ups and other such links that are hosted on foreign servers, effectively sending search queries into the international ether. Americans’ privacy is just as affected by overseas collection as it is by what happens on U.S. soil.

## Corporate surveillance is inevitable and they’ll willingly provide data to the government

Schneier 2015, Berkman Center for Internet and Society at Harvard Law School

[Bruce, Data and Goliath: the Hidden Battles to Collect Your Data and Control Your World, Introduction)]

Corporate surveillance and government surveillance aren’t separate. They’re intertwined; the two support each other. It’s a public-private surveillance partnership that spans the world. This isn’t a formal agreement; it’s more an alliance of interests. Although it isn’t absolute, it’s become a de facto reality, with many powerful stakeholders supporting its perpetuation. And though Snowden’s revelations about NSA surveillance have caused rifts in the partnership—we’ll talk about those in Chapter 14—it’s still strong. The Snowden documents made it clear how much the NSA relies on US corporations to eavesdrop on the Internet. The NSA didn’t build a massive Internet eavesdropping system from scratch. It noticed that the corporate world was already building one, and tapped into it. Through programs like PRISM, the NSA legally compels Internet companies like Microsoft, Google, Apple, and Yahoo to provide data on several thousand individuals of interest. Through other programs, the NSA gets direct access to the Internet backbone to conduct mass surveillance on everyone. Sometimes those corporations work with the NSA willingly. Sometimes they’re forced by the courts to hand over data, largely in secret. At other times, the NSA has hacked into those corporations’ infrastructure without their permission.

This is happening all over the world. Many countries use corporate surveillance capabilities to monitor their own citizens. Through programs such as TEMPORA, the UK’s GCHQ pays telcos like BT and Vodafone to give it access to bulk communications all over the world. Vodafone gives Albania, Egypt, Hungary, Ireland, and Qatar—possibly 29 countries in total—direct access to Internet traffic flowing inside their countries. We don’t know to what extent these countries are paying for access, as the UK does, or just demanding it. The French government eavesdrops on France Télécom and Orange. We’ve already talked about China and Russia in Chapter 5. About a dozen countries have data retention laws—declared unconstitutional in the EU in 2014—requiring ISPs to keep surveillance data on their customers for some months in case the government wants access to it. Internet cafes in Iran, Vietnam, India, and elsewhere must collect and retain identity information of their customers.

Similar things are happening off the Internet. Immediately after 9/11, the US government bought data from data brokers, including air passenger data from Torch Concepts and a database of Mexican voters from ChoicePoint. US law requires financial institutions to report cash transactions of $10,000 or larger to the government; for currency exchangers, the threshold is $1,000. Many governments require hotels to report which foreigners are sleeping there that night, and many more make copies of guests’ ID cards and passports. CCTV cameras, license plate capture systems, and cell phone location data are being used by numerous governments.

By the same token, corporations obtain government data for their own purposes. States like Illinois, Ohio, Texas, and Florida sell driver’s license data, including photos, to private buyers. Some states sell voter registration data. The UK government proposed the sale of taxpayer data in 2014, but public outcry has halted that, at least temporarily. The UK National Health Service also plans to sell patient health data to drug and insurance firms. There’s a feedback loop: corporations argue for more government data collection, then argue that the data should be released under open government laws, and then repackage the data and sell it back to the government.

The net result is that a lot of surveillance data moves back and forth between government and corporations. One consequence of this is that it’s hard to get effective laws passed to curb corporate surveillance—governments don’t really want to limit their own access to data by crippling the corporate hand that feeds them.

# Answers to: Privacy

## No solid proof of chilling effects

**Posner 2013, Prof of Law at U of Chicago**

(Eric, professor at the University of Chicago Law School, is the co-author of "Terror in the Balance" and "The Executive Unbound." “Is the N.S.A. Surveillance Threat Real or Imagined?” 6-9-13. http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined)

This brings me to another valuable point you made, which is that when people believe that the government exercises surveillance, they become reluctant to exercise democratic freedoms. This is a textbook objection to surveillance, I agree, but it also is another objection that I would place under “theoretical” rather than real. Is there any evidence that over the last 12 years, during the flowering of the so-called surveillance state, Americans have become less politically active? More worried about government suppression of dissent? Less willing to listen to opposing voices? All the evidence points in the opposite direction.

Views from the extreme ends of the political spectrum are far more accessible today than they were in the past. It is infinitely easier to get the Al Qaeda perspective today — one just does a Google search — than it was to learn the Soviet perspective 40 years ago, which would have required one to travel to one of the very small number of communist bookstores around the country. It is hard to think of another period so full of robust political debate since the late 1960s — another era of government surveillance.

# Answers to: Encryption

## Myths about encryption and privacy abound

-Encryption can’t overcome determine government; means plan cannot solve.

Kamp 2013, Major computer geek, developed FreeBSD operating system

The Bike Shed (ACM), Vol 11(7), July 30, 2013 “More Encryption Is Not the Solution: Cryptography as privacy works only if both ends work at it in good faith”

The recent exposure of the dragnet-style surveillance of Internet traffic has provoked a number of responses that are variations of the general formula, “More encryption is the solution.” This is not the case. In fact, more encryption will probably only make the privacy crisis worse than it already is. INCONVENIENT FACT #1 ABOUT PRIVACY | Politics Trumps Cryptography Nation-states have police forces with guns. Cryptographers and the IETF (Internet Engineering Task Force) do not. Several nation-states, most notably the United Kingdom, have enacted laws that allow the police to jail suspects until they reveal the cryptographic keys to unlock their computers. Such laws open a host of due process and civil rights issues that we do not need to dwell on here. For now it is enough to note that such laws can be enacted and enforced. INCONVENIENT FACT #2 ABOUT PRIVACY | Not Everybody Has a Right to Privacy The privacy of some strata of the population has been restricted. In many nation-states, for example, prisoners are allowed private communication only with their designated lawyers; all other communications must be monitored by a prison guard. Many employees sign away most of their rights to privacy while “on the clock,” up to and including accepting closed-circuit TV cameras in the company restrooms. Any person can have the right to privacy removed through whatever passes for judicial oversight in their country of residence, so that authorities can confirm or deny a suspicion of illegal activities. People in a foreign country may not have any right to privacy. Depriving them of their privacy is called “espionage,” a fully legal and usually well-funded part of any nation-state’s self-defense mechanism. INCONVENIENT FACT #3 ABOUT PRIVACY| Encryption Will Be Broken, If Need Be This follows directly from the first two points: if a nation-state decides that somebody should not have privacy, then it will use whatever means available to prevent that privacy. Traditionally, this meant intercepting mail, tapping phones, sitting in a flowerbed with a pair of binoculars, installing “pingers,” and more recently, attaching GPS devices to cars. Widely available, practically unbreakable cryptography drastically changed the balance of power, and the 9/11 terrorist attack in New York City 12 years ago acted as a catalyst throughout the world for stronger investigative powers that would allow plans for terrorist activity to be discovered before they could be carried out.

## Successful encryption requires unrealistic cooperation

Kamp 2013, Major computer geek, developed FreeBSD operating system

The Bike Shed (ACM), Vol 11(7), July 30, 2013 “More Encryption Is Not the Solution: Cryptography as privacy works only if both ends work at it in good faith”

In the long run, nobody is going to notice that the symmetric keys are not random—you would have to scrutinize the key material in many thousands of connections before you would even start to suspect something was wrong. That is the basic problem with cryptography as a means of privacy: *it works only if both ends work at it in good faith.*  Major operating-system vendors could be told to collect the keys to encrypted partitions as part of their “automatic update communication,” and nobody would notice that 30-40 extra random-looking bytes got sent back to the mother ship. That would allow any duly authorized officer of the law simply to ask for the passwords, given the machine’s unique identifier. That would be so much more efficient and unobtrusive than jailing the suspect until he or she revealed it. For one thing, the suspects wouldn’t even need to know that their data was under scrutiny

## Terrorism links: Encryption

Washington Post Editorial July 22, 2015

http://www.nhregister.com/opinion/20150722/editorial-putting-the-digital-keys-to-unlock-data-out-of-reach-of-authorities

A contentious debate about encryption of data on smartphones and elsewhere has become even more intense in recent weeks. A collision is unfolding between law enforcement devoted to fighting crime and terrorism and advocates of privacy and secure communications. In these chaotic digital times, both are vital to the national interest, and it is imperative that experts invest serious time and resources into finding ways to reconcile the conflict. FBI Director James Comey has raised alarms — most recently in testimony to Congress this month — about the prospect of law enforcement “going dark,” meaning that it would be unable to obtain information, with a court order, from encrypted communications on smartphones and other sources. The reason for this alarm are the decisions by Apple and Google to provide end-to-end encryption as the default in their operating systems, meaning that only the holder of the device can unlock the information. The technology companies say they do not hold the key (although they do hold data in servers that would still be accessible by law enforcement). Comey warns that this encryption could provide a safe haven for terrorists and criminals. He has not proposed a specific fix, but insisted that the problem of “going dark” is “grave, growing and extremely complex.” Comey’s assertions should be taken seriously. A rule-of-law society cannot allow sanctuary for those who wreak harm

# **Answers to: Free Internet**

## **American open internet agenda is propaganda**

-America looks out for our business first, just like everyone

Hill 2015, Pres. Association for Proper Internet Governance

(Richard, “Dissecting The “Internet Freedom” Agenda” 5-6-15. http://www.ip-watch.org/2015/05/06/book-review-dissecting-the-internet-freedom-agenda/#\_ftn2)

There is a vast literature on internet governance, but much of it is ideological and normative: the author espouses a certain point of view, explains why that point of view is good, and proposes actions that would lead to the author’s desired outcome. There is nothing wrong with that approach: on the contrary, such advocacy is necessary and welcome. But a more detached analytical approach is also needed, and Powers and Jablonski provide exactly that. Their objective is to help us understand (citing from p. 19 of the paperback edition) “why states pursue the policies they do”. The book “focuses centrally on understanding the numerous ways in which power and control are exerted in cyberspace” (p. 19). Starting from the rather obvious premise that states compete to shape international policies that favor their interests, and using the framework of political economy, the authors outline the geopolitical stakes and show how questions of power, and not human rights, are the real drivers of much of the debate about Internet governance. They show how the United States has deliberately used a human rights discourse to promote policies that further its geo-economic and geo-political interests. And how it has used subsidies and government contracts to help its private companies to acquire or maintain dominant positions in much of the ICT sector. Powers and Jablonski dissect the mechanisms by which vibrant government institutions deliberately transferred power to US corporations in order to further US geo-economical and geo-political goals. In particular, they show how a “freedom to connect” narrative is used by the USA to attempt to transform information and personal data into commercial commodities that should be subject to free trade. Yet all states (including the US) regulate, at least to some extent, the flow of information within and across their borders. If information is the “new oil” of our times, then it is not surprising that states wish to shape the production and flow of information in ways that favor their interests. Thus it is not surprising that states such as China, India, and Russia have started to assert sovereign rights to control some aspect of the production and flow of information within their borders, and that European Union courts have made decisions on the basis of European law that affect global information flows and access. As the authors put the matter (p. 6): “the [US] doctrine of internet freedom … is the realization of a broader [US] strategy promoting a particular conception of networked communication that depends on American companies …, supports Western norms …, and promotes Western products.” (I would personally say that it actually supports US norms and US products and services.) As the authors point out, one can ask (p. 11): “If states have a right to control the types of people allowed into their territory (immigration), and how its money is exchanged with foreign banks, then why don’t they have a right to control information flows from foreign actors?” To be sure, any such controls would have to comply with international human rights law. But the current US policies go much further, implying that those human rights laws must be implemented in accordance with the US interpretation, meaning few restrictions on freedom of speech, weak protection of privacy, and ever stricter protection for intellectual property. As Powers and Jablonsky point out (p. 31), the US does not hesitate to promote restrictions on information flows when that promotes its goals. Again, the authors do not make value judgments: they explain how the US deliberately attempts to shape (to a large extent successfully) international policies, so that both actions and inactions serve its interests and those of the large corporations that increasingly influence US policies. The authors also explain how the US military-industrial complex has morphed into an information-industrial complex, with deleterious consequences for both industry and government, consequences such as “weakened oversight, accountability, and industry vitality and competiveness”(p. 23) that create risks for society and democracy. As the authors say, the shift “from adversarial to cooperative and laissez-faire rule making is a keystone moment in the rise of the information-industrial complex” (p. 61). They show how the network effects, economies of scale, and externalities that are fundamental features of the internet favor first-movers, which are mostly US companies. The remedy to such situations is well known: government intervention – widely accepted regarding air transport, road transport, pharmaceuticals, etc., and yet unthinkable for many regarding the internet. But why? As the authors put the matter (p. 24): “While heavy-handed government controls over the internet should be resisted, so should a system whereby internet connectivity requires the systematic transfer of wealth from the developing world to the developed.” But freedom of information is put forward to justify specific economic practices which would not be easy to justify otherwise, for example “no government taxes companies for data extraction or for data imports/exports, both of which are heavily regulated aspects of markets exchanging other valuable commodities”(p. 97). The authors discuss the very current topic of mass surveillance, and its relation to anonymity, showing how, when the US presents the internet and “freedom to connect” as analogous to public speech and town halls, it is deliberately arguing against anonymity and against privacy – and this of course in order to avoid restrictions on its mass surveillance activities. Thus the authors posit that there are tensions between the US call for “internet freedom” and other states’ calls for “information sovereignty”, and analyze the 2012 World Conference on International Telecommunications from that point of view. Not surprisingly, the authors conclude that international cooperation, recognizing the legitimate aspirations of all the world’s peoples, is the only proper way forward. As the authors put the matter (p. 206): “Activists and defenders of the original vision of the Web as a ‘fair and humane’ cyber-civilization need to avoid lofty ‘internet freedom’ declarations and instead champion specific reforms required to protect the values and practices they hold dear.” And it is with that in mind, as a counterweight to US and US-based corporate power, that a group of civil society organizations have launched the Internet Social Forum.

## Many issues undermine US internet leadership

-passing the plan is not enough to overcome other causes

Eades 2013, American author and teacher

(Mark, American writer and educator currently residing in Shanghai, China. He has taught at both Shanghai International Studies University and Fudan University. 7-17-13. “Western Governments Lose Credibility as Global Surveillance Scandal Grows” http://www.atlantic-community.org/-/western-governments-lose-credibility-as-global-surveillance-scandal-grows)

As revelations of secret surveillance programs by Western governments appear almost daily and the drama of American whistleblower Edward Snowden's bid for freedom continues to unfold, the governments of the US and its Western allies are quickly losing credibility globally. In order to regain credibility, the West must come clean about its global surveillance activities, take steps to cease or at least significantly reduce such activities, and end persecution of whistleblowers such as Snowden. Ongoing reveals from former US National Security Agency (NSA) analyst Edward Snowden implicate the US and other Western governments in spying and surveillance activities that appear to violate the rights of citizens and go far beyond the bounds of national security interests. These revelations, and America's relentless pursuit of Snowden with the acquiescence of European governments, have severely damaged the credibility of Western governments internally and externally. Chief among the offending parties is the US, whose extensive domestic and global surveillance activities include monitoring civilian internet, e-mail, and telephone use, both within the US and around the world, as well as spying on European Union diplomats. The revelation that the US has been spying on innocent civilians domestically and internationally, as well as on its EU allies, undercuts America's insistence that such activities are carried out only as necessary for national security. It also severely tarnishes America's image as a champion of democracy, human rights, and civil liberties. US accusations of spying and computer hacking by countries like China will now likely fall on deaf ears. Simply put, America has come off looking like a hypocrite. America's chief partner in crime in these activities is the United Kingdom. Documents released by Snowden reveal that the UK's Government Communications Headquarters (GCHQ) spied on delegates at the 2009 G-20 summit in London and has been intercepting and storing mass quantities of fiber-optic internet traffic in concert with the NSA. The German government has also been implicated in NSA spying on German citizens. Reports unrelated to Snowden have further revealed that France's intelligence agency, the General Directorate for External Security (DGSE), has been using NSA-style methods to spy on the internet use, e-mail, and telephone communications of French citizens. These revelations have led many to conclude that we are now living in the era of the "Global Surveillance State." The subjects of alleged Western spying activities are not mainly rogue states or terrorist groups, but ordinary private citizens and allies. The prominent and highly profitable role played by private security firms in these activities, at public expense, increases suspicion that spying is motivated by more than just national security interests. In an age of austerity, the taxpayers of Western nations are paying their own governments to spy on them, at great profit to the security firms doing the spying. Public services may suffer, but corporate spies are handsomely paid from the public coffers. Meanwhile, the pursuit of Snowden increasingly seems vindictive and foolish as the US relentlessly pressures other countries to cooperate. Feigning nonchalance on the matter in public as a face-saving measure, the US works feverishly behind the scenes to capture Snowden and make an example of him for other would-be whistleblowers. Recently an airplane carrying Bolivian president Evo Morales from Russia to Bolivia was turned away from France and Portugal and grounded in Vienna for ten hours because it was suspected that Snowden might be on board. Snowden was not aboard Morales's flight, and Latin Americans were enraged by the incident. Despite expressed outrage at the alleged

## America’s TPP agenda destroys Free Internet

Nevins 2015, Foreign affairs journalist from MintPress

(Sean, “The TPP Threatens A Free And Open Internet” May 7, 2015, http://www.mintpressnews.com/the-tpp-could-curtail-internet-freedom-national-sovereignty-free-open-internet/205383/)

Legislation to “fast track” the Trans-Pacific Partnership (TPP) has moved through both committees in the House and the Senate. This legislation, which would enable President Barack Obama to negotiate the terms of the international agreement without congressional input, is now on the floor of the House. While the TPP has come under increasing scrutiny for its potential to erode the sovereignty of countries, an often overlooked aspect of the treaty is its threat to a free and open Internet. “The Trans-Pacific Partnership is pushing the worst parts of U.S. copyright policy on the rest of the world without expanding protections for fair use,” said Evan Greer, campaign manager with Fight for the Future, an organization dedicated to protecting Internet freedoms. Speaking to MintPress News, Greer explained that the TPP has the potential to create a system in which content could be censored with a copyright claim without maintaining basic protections to protect freedom of speech and innovation on the Internet. This could potentially allow copyright laws to be used by powerful institutions to pull down legitimate free speech on the Internet. Yet Greer also acknowledged that nothing about the TPP is known for sure. “The fundamental problem here is that we don’t know enough about it to know how it might affect us,” he said. “That’s one of the biggest problems. Internet users should have a say and a voice to access policy when it affects them.” SOPA and the TPP Fight for the Future formed in the lead up to fight the Stop Online Piracy Act (SOPA) and PROTECT IP Act (PIPA) in 2012. Aiming to combat copyright infringement, those acts were promoted by Hollywood entertainment companies to censor websites caught broadcasting their content. However, the legislation would have enabled law enforcement to wield much larger powers. The Electronic Frontier Foundation explains: “Although the bills were ostensibly aimed at reaching foreign websites dedicated to providing illegal content, their provisions would allow for removal of enormous amounts of non-infringing content including political and other speech from the Web.” Fight for the Future was instrumental in launching the SOPA Strike, the largest online protest in history. An array of companies and personal websites participating blacked out their websites for 12 hours on Jan. 18, 2012, many using Fight for the Future’s online tools. Some of those companies included Internet giants like Google, WordPress, Wikipedia and Flickr. There is a direct line from SOPA to the TPP. Some of the same Hollywood lobbying firms that helped to write legislation and promote SOPA are now working on the Internet copyright chapter of the TPP, according to Greer. These firms include the Recording Industry Association of America and the Motion Picture Association of America. “Essentially, after SOPA they realized they were never going to be able to get these draconian laws passed publically, so they’ve been trying to get them pushed into these secretive trade agreements,” Greer said. According to the EFF, the TPP could potentially criminalize Internet users for non-commercial activities like file sharing. The organization, which works to defend civil liberties in the digital world, explained that the United States is attempting to put language in the treaty that would criminalize anyone who publishes work on a “commercial scale,” with penalties including prison and hefty monetary fines. EFF explains the problem with the text’s language: “As anyone who has ever had a meme go viral knows, it is very easy to distribute content on a commercial scale online, even without it being a money-making operation. That means fans who distribute subtitles to foreign movies or anime, or archivists and librarians who preserve and upload old books, videos, games, or music, could go to jail or face huge fines for their work. Someone who makes a remix film and puts it online could be under threat. Such a broad definition is ripe for abuse, and we’ve seen such abuse happen many times before.”

## Corporate surveillance wrecks internet freedom

Schneier 2015, Berkman Center for Internet and Society at Harvard Law School

[Bruce, Data and Goliath: the Hidden Battles to Collect Your Data and Control Your World, Introduction)]

Most of the big US defense contractors, such as Raytheon, Northrop Grumman, and Harris Corporation, build cyberweapons for the US military. And many big IT companies help build surveillance centers around the world. The French company Bull SA helped the Libyan government build its surveillance center. Nigeria used the Israeli firm Elbit Systems. Syria used the German company Siemens, the Italian company Area SpA, and others. The Gadhafi regime in Libya purchased telephone surveillance technology from China’s ZTE and South Africa’s VASTech. We don’t know who built the Internet surveillance systems used in Azerbaijan and Uzbekistan, but almost certainly some Western companies helped them. There are few laws prohibiting this kind of technology transfer, and the ones that exist are easily bypassed.

These are not only specially designed government eavesdropping systems; much government surveillance infrastructure is built for corporate use. US-based Blue Coat sells monitoring and content filtering systems for corporate networks, which are also used for government surveillance in countries like Burma, China, Egypt, Indonesia, Nigeria, Qatar, Saudi Arabia, Turkey, and Venezuela. Netsweeper is a Canadian corporate filtering product used for censorship by governments in Qatar, Yemen, the UAE, Somalia, and Pakistan. Filtering software from the US company Fortinet is used to censor the Internet in Burma; SmartFilter, from the US company McAfee and normally used in schools, helps the governments of Tunisia and Iran censor the Internet in their countries. Commercial security equipment from the UK company Sophos has been used by Syria and other oppressive regimes to surveil and arrest their citizens.

Technology is value neutral. You can use your phone to call 911 or to plan a bank robbery. There’s no technical difference between a government’s using a tool to identify criminals or using it to identify dissidents. There’s no technical difference between corporate and government uses. Legitimate corporate tools for blocking employees from e-mailing confidential data can be used by repressive governments for surveillance and censorship. Conversely, the same anti-censorship tools that Saudi and Iranian dissidents use to evade their governments can be used by criminals to distribute child porn. Encryption allows the good guys to communicate without being eavesdropped on by the bad guys, and also allows the bad guys to communicate without being eavesdropped on by the good guys. And the same facial recognition technology that Disney uses in its theme parks to pick out photos its patrons might want to buy as souvenirs can identify political protesters in China, and Occupy Wall Street protesters in New York.

Critique link: Affirmative is a diversionary irrelevance:

-surveillance and lawlessness too-deeply embedded

-Congressional action cannot curtail surveillance

Whitehead, President of Rutherford Institute 2015 John, President Rutherford Institute, “Free Speech, Facebook and the NSA: The Good the Bad the Ugly”, HuffPo, 4 June 2015 <http://www.huffingtonpost.com/john-w-whitehead/free-speech-facebook-and-_b_7497064.html> In other words, telephone surveillance by the NSA is the least of our worries. Even with restrictions on its ability to collect mass quantities of telephone metadata, the government and its various spy agencies, from the NSA to the FBI, can still employ an endless number of methods for carrying out warrantless surveillance on Americans, all of which are far more invasive than the bulk collection program. As I point out in my new book *Battlefield America: The War on the American People*, just about every branch of the government -- from the Postal Service to the Treasury Department and every agency in between -- now has [its own surveillance sector](https://nsa.gov1.info/partners/index.html), authorized to spy on the American people. Just recently, for example, it was revealed that the FBI has been employing a [small fleet of low-flying planes](http://www.usnews.com/news/politics/articles/2015/06/02/fbi-behind-mysterious-surveillance-aircraft-over-us-cities) to carry out video and cell phone surveillance over American cities. Then there are the fusion and counterterrorism centers that gather all of the data from the smaller government spies -- the police, public health officials, transportation, etc. -- and make it accessible for all those in power. And of course, that doesn't even begin to touch on the complicity of the corporate sector, which buys and sells us from cradle to grave, until we have no more data left to mine. Indeed, [Facebook, Amazon and Google](http://articles.latimes.com/2013/jun/30/nation/la-na-consumer-tracking-20130701) are among the government's closest competitors when it comes to carrying out surveillance on Americans, monitoring the content of your emails, tracking your purchases and exploiting your social media posts. "Few consumers understand what data are being shared, with whom, or how the information is being used," reports the [*Los Angeles Times*](http://articles.latimes.com/2013/jun/30/nation/la-na-consumer-tracking-20130701). "Most Americans emit a stream of personal digital exhaust -- what they search for, what they buy, who they communicate with, where they are -- that is captured and exploited in a largely unregulated fashion." It's not just what we say, where we go and what we buy that is being tracked. We're being surveilled right down to our genes, thanks to a potent combination of hardware, software and data collection that scans our biometrics -- our faces, irises, voices, genetics, even our gait -- runs them through computer programs that can break the data down into unique "identifiers," and then offers them up to the government and its corporate allies for their respective uses. All of those internet-connected gadgets we just have to have (*Forbes* refers to them as["(data) pipelines to our intimate bodily processes"](http://www.forbes.com/sites/jmaureenhenderson/2015/01/06/dystopia-digital-detoxes-and-how-black-mirror-helps-us-make-sense-of-the-apple-watch/)) -- the smart watches that can monitor our blood pressure and the smart phones that let us [pay for purchases](http://www.smithsonianmag.com/innovation/forget-credit-cards-now-you-can-pay-your-eyes-180955445/) with our fingerprints and iris scans -- are setting us up for a brave new world where there is nowhere to run and nowhere to hide. For instance, imagine what the NSA could do (and might already be doing) with voiceprint technology, which has been likened to a fingerprint. Described as "the next frontline in the battle against overweening public surveillance," the collection of voiceprints is a booming industry for governments and businesses alike. As [The Guardian reports](http://www.theguardian.com/technology/2014/oct/13/rise-voiceprint-id-technology-privacy-campaigners-concerned), "voice biometrics could be used to pinpoint the location of individuals. There is already discussion about placing voice sensors in public spaces, and Lee Tien, senior staff attorney with the Electronic Frontier Foundation, said that multiple sensors could be triangulated to identify individuals and specify their location within very small areas." Suddenly the NSA's telephone metadata program seems like child's play compared to what's coming down the pike. That, of course, is the point. Whatever recent victories we've enjoyed -- the [Second Circuit ruling](http://www.politico.com/story/2015/05/nsa-phone-data-collection-illegal-court-ruling-117725.html) declaring the NSA's metadata program to be illegal, [Congress' inability](http://www.scmagazine.com/usa-freedom-act-fails-to-pass-and-section-215-sunsets/article/418018/) to reauthorize Section 215 of the Patriot Act, even the [Supreme Court's recognition](http://www.cnn.com/2015/06/01/politics/supreme-court-elonis-facebook-ruling/) that free speech on the internet may be protected -- amount to little in the face of the government's willful disregard of every constitutional safeguard put in place to protect us from abusive, intrusive government agencies out to control the populace. Already, the American people are starting to lose interest in the spectacle of Congress wrangling, debating and negotiating over the NSA and the Patriot Act. Already, the media outlets are being seduced by other, more titillating news: [Caitlyn Jenner's](http://www.cnn.com/2015/06/01/entertainment/bruce-caitlyn-jenner-vanity-fair-feat/index.html) *Vanity Fair* cover, Kim Kardashian's [pregnancy](http://www.huffingtonpost.com/2015/05/31/kim-kardashian-pregnant-second-child_n_6096624.html) announcement, and the new *Fifty Shades of Grey* book told from [Christian's](http://www.cnn.com/2015/06/01/entertainment/fifty-shades-grey-new-christian-feat/index.html) perspective. What remains to be seen is whether, when all is said and done, the powers-that-be succeed in distracting us from the fact that the government's unauthorized and unwarranted surveillance powers go far beyond anything thus far debated by Congress or the courts.

## No need for plan: Freedom Act strong enough signal on internet governance

Hogan Lovells June 2015

[Hogan Lovells and its team of 60-plus lawyers from the Privacy and Information Management Group are proud to be contributors to the International Association of Privacy Professionals’ Tracker Blog. The Privacy Team the likes of Harriet Pearson, Daniel Solove, Marcy Wilder and Christopher Wolf., June 25, 2015, “ USA FREEDOM Act: A Step Toward Restoring Trust? https://privacyassociation.org/about/person/003a0000029gOLSAA2

Regardless of one’s views on the merits of the legislation, however, enactment of the USA FREEDOM Act does appear to have the potential to benefit U.S. industry.   As the nature and scope of U.S. government surveillance practices increasingly came to light in the past few years, U.S. electronic communications service providers were sometimes—and often unfairly—criticized for their involvement with surveillance under the USA PATRIOT Act and FISA. That criticism has had a dramatic impact, especially outside the U.S. In the EU, the revelations led in part to a full-blown review and renegotiation of the EU-U.S. Safe Harbor agreement, which enables compliant data flows between the EU and certified companies in the U.S. This ongoing review and renegotiation has created substantial uncertainty for those companies that rely on Safe Harbor to facilitate the EU-U.S. data transfers essential to their day-to-day operations. Reports of U.S. government surveillance also were used to support efforts in Latin America, Europe and Russia to establish data-localization laws. Some European stakeholders, including politicians, have positioned EU privacy rules as a competitive advantage for European service providers. Several service providers outside the U.S. now promise that data will never be sent to U.S.-based sub-processors or data centers. Some analysts even projected that the U.S. digital-services sector would lose billions of dollars as a result of overseas customers moving their data to local service providers believed to be outside the reach of the U.S. surveillance apparatus. Electronic communications service providers faced these difficulties in spite of the fact that other countries, including many in the EU, [engage in surveillance](https://privacyassociation.org/news/a/is-personal-data-better-protected-from-government-surveillance-in-europe-th) similar to that conducted in the U.S. under FISA and the USA PATRIOT Act and in many cases with [more expansive and unchecked government power](http://www.hldataprotection.com/files/2013/05/A-Sober-Look-at-National-Security-Access-to-Data-in-the-Cloud.pdf). But now that the U.S. government has shown its willingness to evaluate and reform its surveillance practices, the path to finalizing the Safe Harbor negotiations may become more clear. For example, U.S. service providers can point to the reforms in the USA FREEDOM Act when addressing concerns about government access to data. And the European Court of Justice may refer to the USA FREEDOM Act in a positive light when ruling on the validity of Safe Harbor in the *Schrems v. Irish Data Protection Commissioner* case.